Certificate Authority (CA) Auditing

WebTrust™ for Certificate Authorities

June 2000

Agenda

- Why Audit?
- Why Use an Accounting Firm?
- CA Auditing in the 20th Century
- CA Auditing in the 21st Century
- Principles and Criteria
- The WebTrust *Seal of Approval*
- WebTrust CA Audit ROM
- References

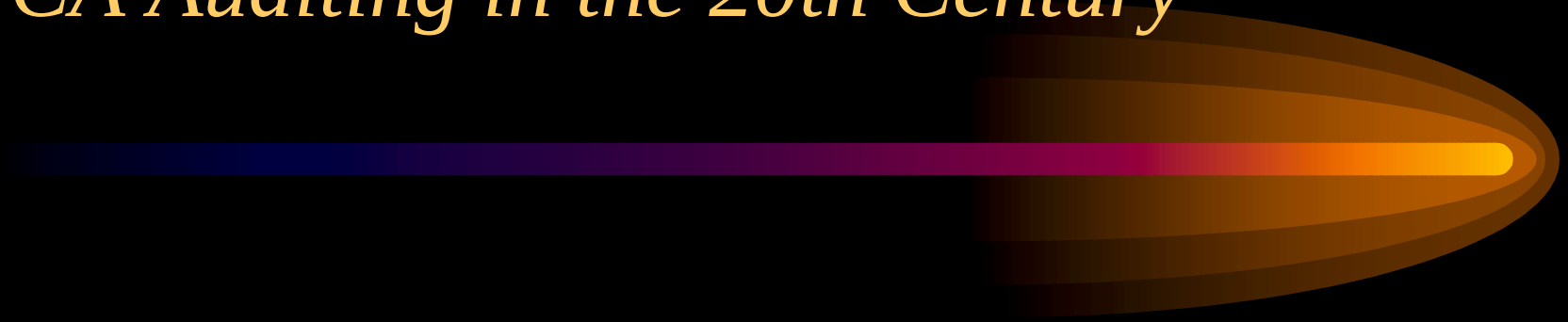
Why Audit?

- provides an external opinion on the completeness of a system against it’s stated goals (e.g., requirements)
- provides for an unbiased evaluation
- can uncover errors before they impact operations, or result in fiscal or physical damage
- verifies that internal controls are in place to mitigate the risk of fraud
- can reduce risks and liabilities
- provides a measure of assurance and comfort to the client

Why Use an Accounting Firm?

- Guidance provided by the American Institute of Certified Public Accountants (AICPA)
- Professional Qualifications (CPA)
- Knowledge of:
  - Generally Accepted Accounting Practices (GAAP)
  - Generally Accepted Auditing Standards (GAAS)
- Unbiased, Independent Third-Party
- Detailed Reports that can be Published and Distributed to Clients

CA Auditing in the 20th Century



The Way It Was ...

Statement on Auditing Standards (SAS) No. 70 Report

- Form and content specified by the American Institute of Certified Public Accountants (AICPA)
- The SAS 70 Report has been used for PKI Audits because a Certificate Authority (CA) is involved with:
  - "Executing transactions and maintaining the related accountability...
  - …recording transactions and processing related data" (a)
- However, the SAS 70 was originally meant for use "when auditing the financial statements of an entity that uses a service organization to process certain transactions." (b)
- Until WebTrust, the SAS 70 Report was all we had!

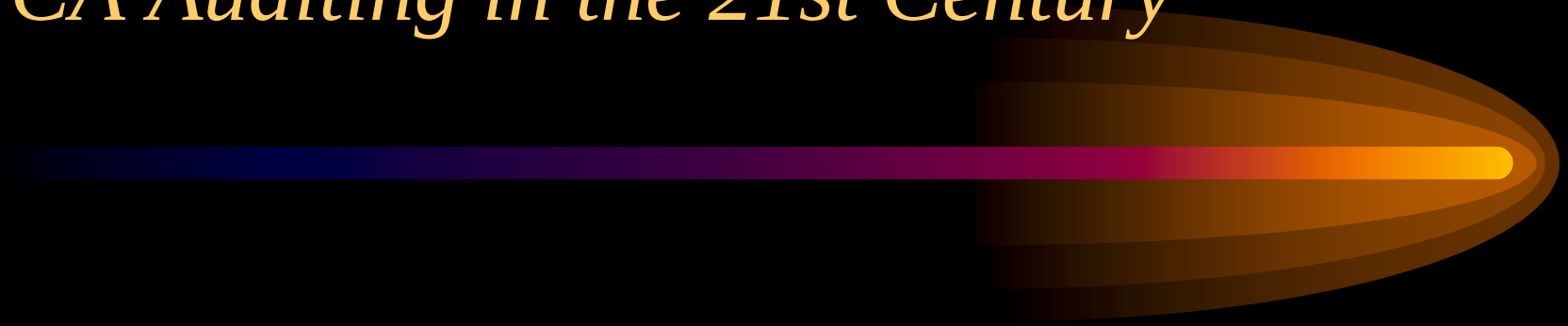
Type I Audit

- A Type I Audit does not include any actual testing. It consists of documentation reviews, employee interviews, and procedural reviews
- A Type I Audit determines only that:
  - the accompanying description presents fairly the aspects of Certificate Authority (CA) controls that may be relevant to a client (i.e., customer) organization's internal controls
  - the controls included in the description were suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily
  - such controls had been placed in operation as of a specific (i.e., a single point in time)

Type II Audit

- A Type II Audit consists of all aspects of a Type I Audit plus:
  - tests are applied to specific controls to obtain evidence about their effectiveness in meeting the related control objectives
  - the observations and tests cover a date *range* (i.e., a period of time versus a single point in time)
  - specific controls, nature, timing, extent, and results of the tests are listed in the Report
- However:
  - no procedures are performed to evaluate the effectiveness of controls at individual client organizations

CA Auditing in the 21st Century



… The Way It Will Be

Advantages of WebTrust

- Since the SAS No. 70 Service Auditor's Report is not adequate for, or targeted to, the audit of a Certificate Authority, the *WebTrust for Certificate Authorities* program was undertaken by the AICPA & CICA
- *WebTrust Principles and Criteria for Certificate Authorities* provides robust auditing guidelines specifically tailored for Certificate Authorities
- *WebTrust for Certificate Authorities* provides a Seal Program that assures customers that the Certification Authority has robust policies that are tested continuously

Guidance Document

- The American Institute of Certified Public Accountants (AICPA) and the Chartered Accountants of Canada (CICA) have collaborated on the *WebTrust Principles and Criteria for Certification Authorities*.
- An Exposure Draft has been released for public comment
- The stated goal are:
  - provide a framework for licensed WebTrust practitioners to assess the adequacy and effectiveness of the controls employed by Certification Authorities
  - support the growing demand for third-party authentication
  - provide assurance with respect to e-commerce business activities

Comparing WebTrust to SAS 70 (c)

1. Purpose
2. Target of Evaluation
3. Type of Engagement
4. Examination Standards
5. Coverage of Activities
6. Linkage to Authoritative Standards
7. Period of Coverage of Review

1. Purpose

WebTrust for Certificate Authorities provides a new framework for reporting activities of CAs through auditor communication to interested parties including business partners and existing or potential customers. SAS No. 70 was designed for auditor-to-auditor communications to assist the user auditor in reporting on the financial statements of a customer of the service organization.

2. Target of Evaluation

WebTrust for Certification Authorities was designed specifically for the examinations of CA business activities. Service auditor reports were designed for service organizations in general.

3. *Type of Engagement*

WebTrust for Certificate Authorities requires reporting on compliance with the AICPA/CICA *WebTrust Principles and Criteria for Certification Authorities*. Service auditor reports were designed for *reporting to other auditors* on the design and existence of controls (SAS 70 Type I) and the effective operation of those controls when the report covers a period of time (SAS 70 Type II).

4. Examination Standards

WebTrust for Certificate Authorities follows the Statements on Standards for Attestation Engagements (U.S.) and Standards for Assurance Engagements (Canada). Service auditor reports follow generally accepted auditing standards.

5. *Coverage of Activities*

WebTrust for Certificate Authorities requires coverage of specific areas defined by the AICPA/CICA *WebTrust Principles and Criteria for Certificate Authorities*, including CA business practices disclosure, service integrity (including key and certificate life cycle management activities), and CA environmental controls. Service auditor reports were designed for reporting on controls related specifically to financial information.

6. Linkage to Authoritative Standards

WebTrust for Certificate Authorities provides uniform standards derived from the draft X9.79 standard (which is intended to be submitted to the International Standards Organization (ISO) for international standardization). Standards underlying service auditor reports do not specify the control objectives that must be covered by the report.

7. Period of Coverage of Review

WebTrust for Certificate Authorities requires continuous coverage from the point of initial qualification. Qualification after compliance can be tested over a minimum two-month period, with updates over a specified period (currently one-year maximum). Service auditor reports cover a period of time specified by the service organization, but do not require continuous coverage.

Differences At a Glance

Content/Approach	**AICPA SAS No. 70**	**WebTrust**
Purpose	Auditor to Auditor Communications	Auditor Communications to Interested Parties
Target of Evaluation	Defined by Each Engagement	CA Business Activities Predefined
Type of Engagement	Report on Controls Placed in Operation	Report on Compliance based on WebTrust Criteria
Examination Standards	Generally Accepted Auditing Standards	Standards for Attestation Engagements (U.S.)
Coverage of Activities	No Mandatory Coverage	CA Business Practice Disclosure, Service Integrity, and Environmental Controls
Authoritative Standards	Adequacy of Control Objectives Subjectively Determined by Auditor	Principles and Criteria Linked to ANSI X9.79 Standard. AICPA Provides Uniform Standards
Period of Coverage	Type I (Point in Time) or Type II (Period of Time)	Continuous Coverage From the Point of Qualification.

Principles and Criteria

Some of the control objectives
for a WebTrust CA Audit

CA Business Practices Disclosure

- Identification of each CP and CPS for which the CA issues certificates
- Community and applicability, including a description of the types of entities within the PKI and the applicability of certificates issued by the CA
- Contact details and administrative provisions, including:
  - Contact person
  - Identification of Policy Authority
  - Street address
  - Version and effective date(s) of each CP and CPS
- Any applicable provisions regarding apportionment of liability
- Financial responsibility, including:
  - Indemnification by relying parties
  - Fiduciary relationships
- Interpretation and enforcement, including:
  - Governing law
  - Severability, survival, merger, and notice
  - Dispute resolution procedures

CA Business Practices Disclosure (cont'd)

- Fees, including:
  - Certificate issuance or renewal fees
  - Certificate access fees
  - Revocation or status information access fees
  - Fees for other services such as policy information
  - Refund policy
- Publication and repository requirements, including:
  - Publication of CA information
  - Frequency of publication
  - Access controls
- Compliance audit requirements including:
  - Frequency of entity compliance audit
  - Identity and qualifications of auditor
  - Auditor's relationship to audited party
  - Topics covered by audit
  - Actions taken as a result of deficiency
  - Communication of results

CA Business Practices Disclosure (cont'd)

- Description of the conditions for applicability of certificates issued by the CA that reference a specific Certificate Policy, including:
  - Specific permitted uses for the certificates if such use is limited to specific applications
  - Limitations on the use of certificates if there are specified prohibited uses for such certificates
- Repository obligations, including:
  - Timely publication of certificates and Certificate Revocation Lists
- CA and/or RA obligations:
  - Notification of issuance of a certificate to the subscriber who is the subject of the certificate being issued
  - Notification of issuance of a certificate to others than the subject of the certificate
  - Notification of revocation or suspension of a certificate to the subscriber whose certificate is being revoked or suspended
  - Notification of revocation or suspension of a certificate to others than the subject whose certificate is being revoked or suspended.

CA Business Practices Disclosure (cont'd)

- RA obligations, including:
  - Identification and authentication of subscribers
  - Validation of revocation and suspension requests
  - Verification of subscriber renewal or rekey requests
- Subscriber obligations, including:
  - Accuracy of representations in certificate application
  - Protection of the subscriber's private key
  - Restrictions on private key and certificate use
  - Notification upon private key compromise
- Relying party obligations, including:
  - Purposes for which certificate is used
  - Digital signature verification responsibilities
  - Revocation and suspension checking responsibilities
  - Acknowledgment of applicable liability caps and warranties
- Any applicable reliance or financial limits for certificate usage

CA Business Practices Disclosure (cont'd)

Key Life Cycle Management

- CA Key Generation
- CA Key Storage, Backup and Recovery
- CA Public Key Distribution
- CA Key Escrow
- CA Key Usage
- CA Key Destruction
- CA Key Archival
- CA Cryptographic Hardware Life Cycle Management
- CA-Provided Subscriber Key Management Services

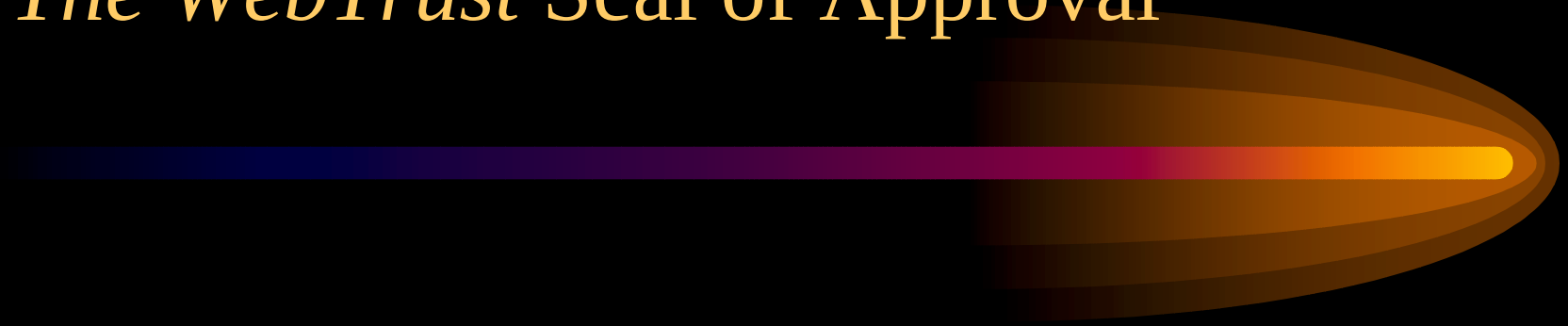
Certificate Life Cycle Management

- Subscriber Registration
- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Suspension
- CRL Processing
- Smart Card Life Cycle Management

CA Environmental Controls

- CPS and CP Management
- Security Management
- Asset Classification and Management
- Personnel Security
- Physical and Environmental Security
- Business Continuity Management
- Operations Management
- System Access Management
- Systems Development and Maintenance
- Monitoring and Compliance
- Event Journaling

The WebTrust Seal of Approval



Obtaining a WebTrust Seal

The CA management must have:

- disclosed key and certificate life cycle management business and information privacy practices, and provided its services in accordance with those practices
- maintained effective controls to provide reasonable assurance that the integrity of the keys and certificates it manages is established and protected throughout their life cycles

Obtaining a WebTrust Seal (continued)

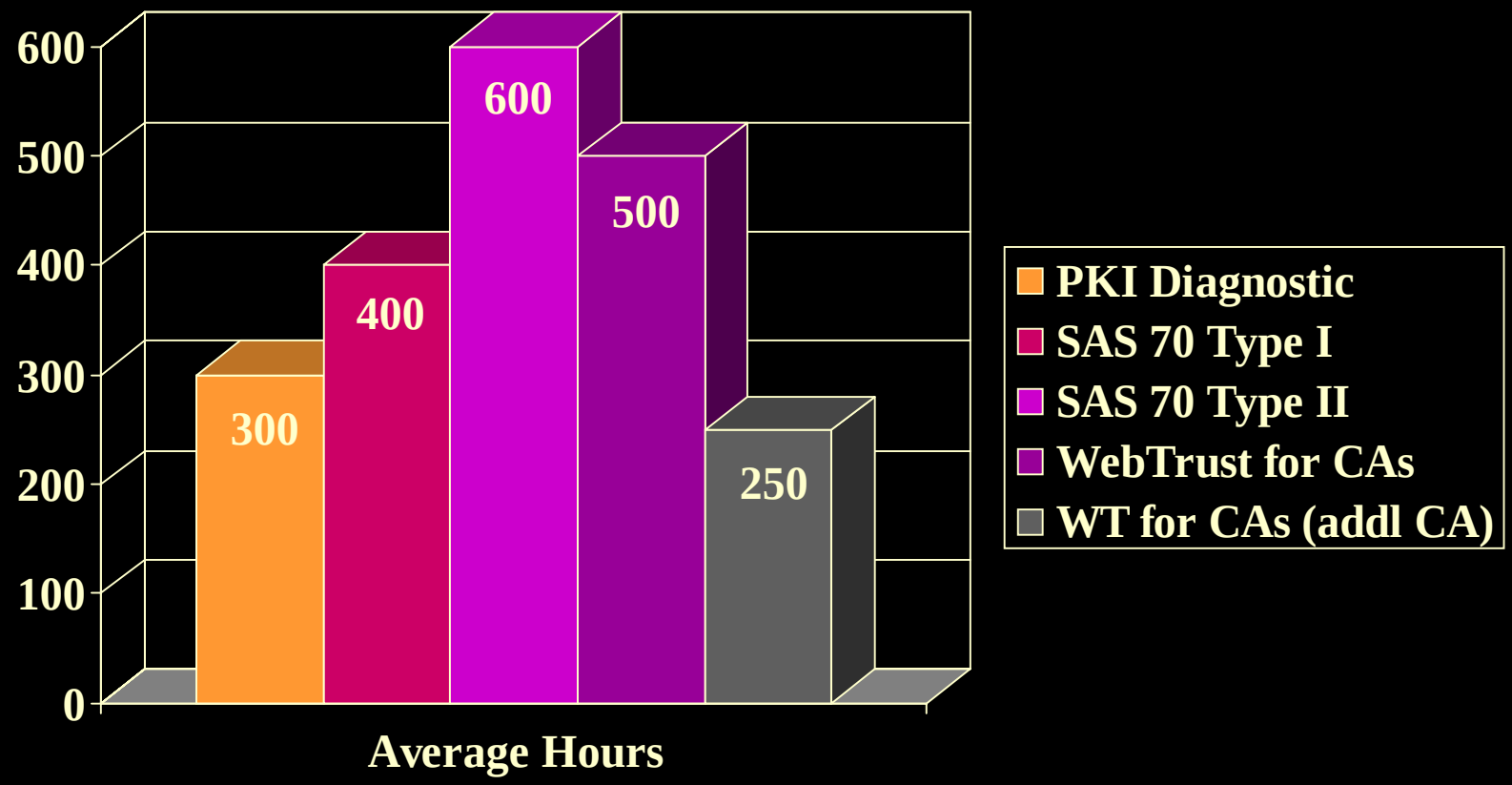
- maintained effective controls to provide reasonable assurance that:
  - subscriber and relying party information is properly authenticated, restricted to authorized individuals, and protected from uses not related to the CA's business
  - the continuity of key and certificate life cycle management operations is maintained
  - systems development, maintenance, and operation are properly authorized and performed to maintain CA systems integrity
- demonstrated compliance for a historical period.

Keeping a WebTrust Seal

- Once the historical period is met, and the compliance is demonstrated (e.g., a WebTrust Audit), the *WebTrust Seal* is issued
- The *WebTrust Seal* resides on the WebTrust server and is displayed on the CA Website via an HTTP link
- Clicking on the *WebTrust Seal* will provide information to the user and/or relying party regarding WebTrust Seal award date, independent Auditor, etc.
- Failure to maintain the rigorous WebTrust criteria will result in the link to the Seal being terminated.

WebTrust CA Audit ROM

CA Audits - Level of Effort



References

AICPA Contact

- The AICPA/CICA *WebTrust Principles and Criteria for Certification Authorities* exposure draft may be viewed at:

  <http://www.aicpa.org/webtrust/caexec~1.htm>.

- Comments on this exposure draft may be sent to Sheryl Weiner, WebTrust Team Leader, Assurance Services, AICPA, 1211 Avenue of the Americas, New York, NY 10036-8775. Responses may also be sent by electronic mail via to sweiner@aicpa.org.

References

(a) AICPA Professional Standards, Volume 1, U.S. Auditing Standards, Attestation Standards, as of June 1, 1996, page AU§324.03.

(b) AICPA Professional Standards, Volume 1, U.S. Auditing Standards, Attestation Standards, as of June 1, 1996, page AU§324.02.

(c) Exposure Draft of the AICPA/CICA WebTrust SM/TM Principles and Criteria for Certification Authorities

For More Information:

Charlie Scruggs
KPMG LLP
2001 M Street, NW
Washington, DC 20036
Voice: 202-533-5806
E-mail: cscruggs@kpmg.com